

10

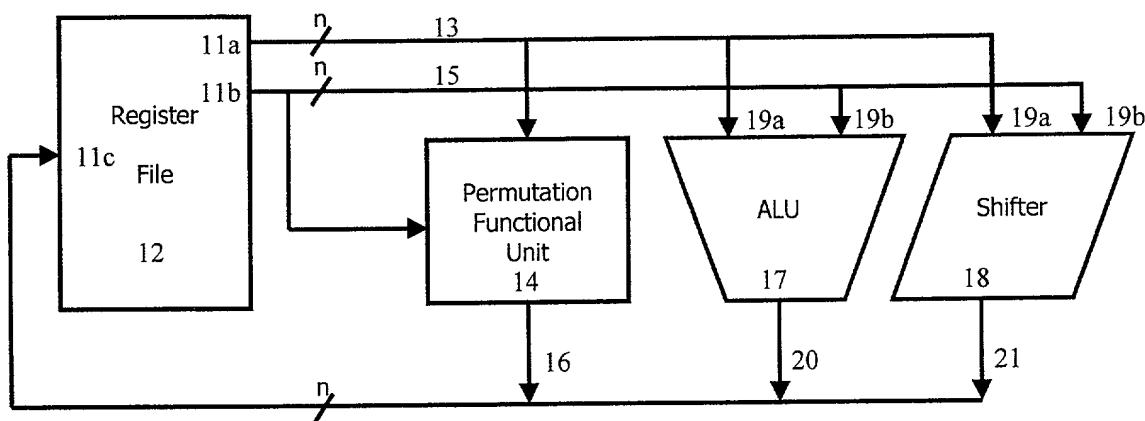


FIG. 1

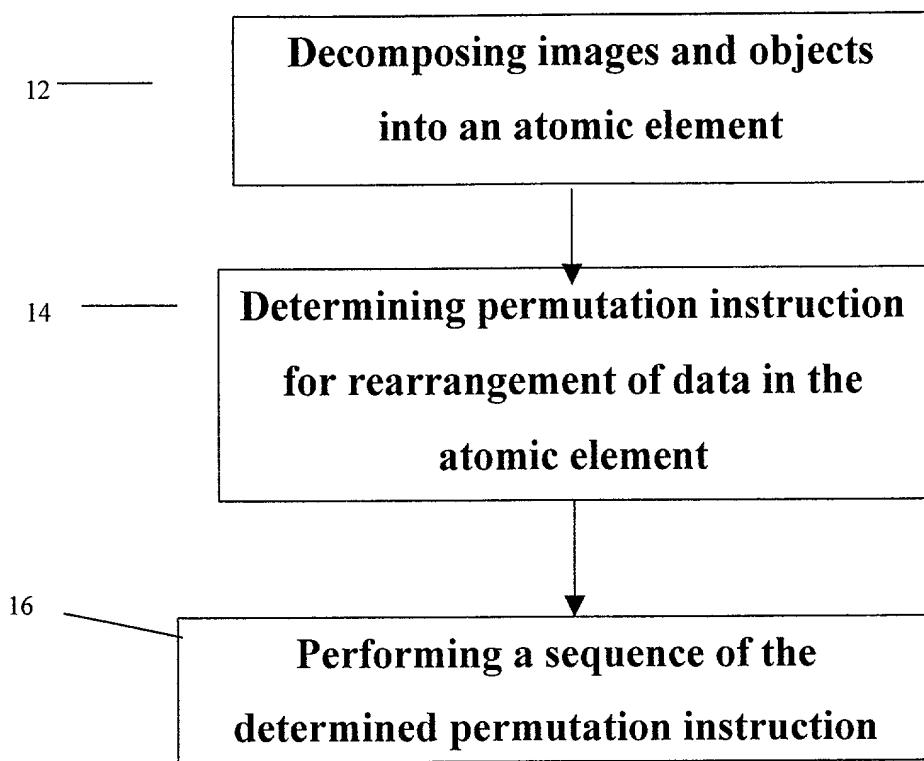


FIG. 2

(a) Area mapping of a 4x4 matrix:

R1 =	a00	a01	a02	a03
R2 =	a10	a11	a12	a13
R3 =	a20	a21	a22	a23
R4 =	a30	a31	a32	a33

Fig. 3a

(b) Decomposition into four 2x2 matrices:

R1 =	a00	a01	b00	b01
R2 =	a10	a11	b10	b11
R3 =	c00	c01	d00	d01
R4 =	c10	c11	d10	d11

Fig. 3B

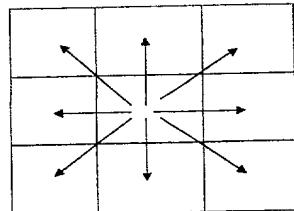


Fig. 4A

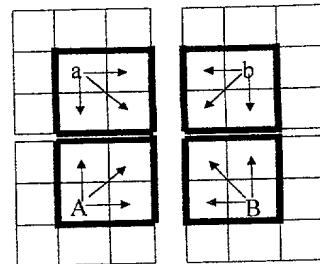


Fig. 4B

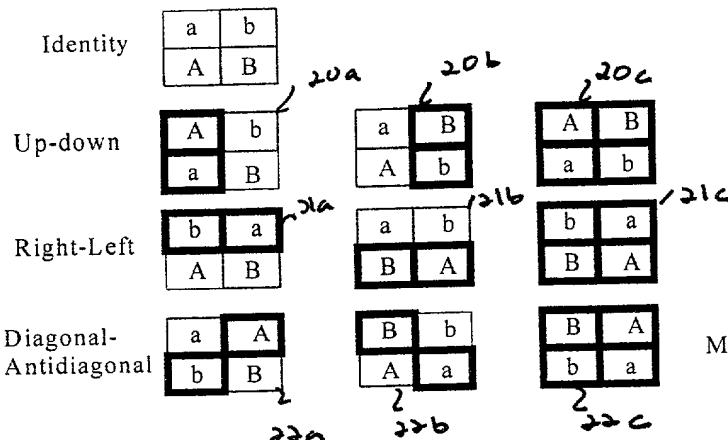
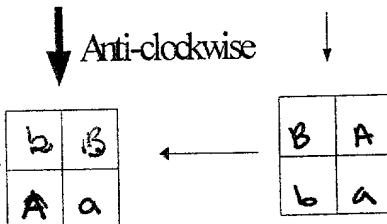
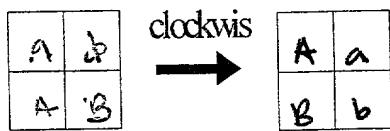


Fig. 4C



Rotate by 2 elements
= swap diagonal and
antidiagonal elements

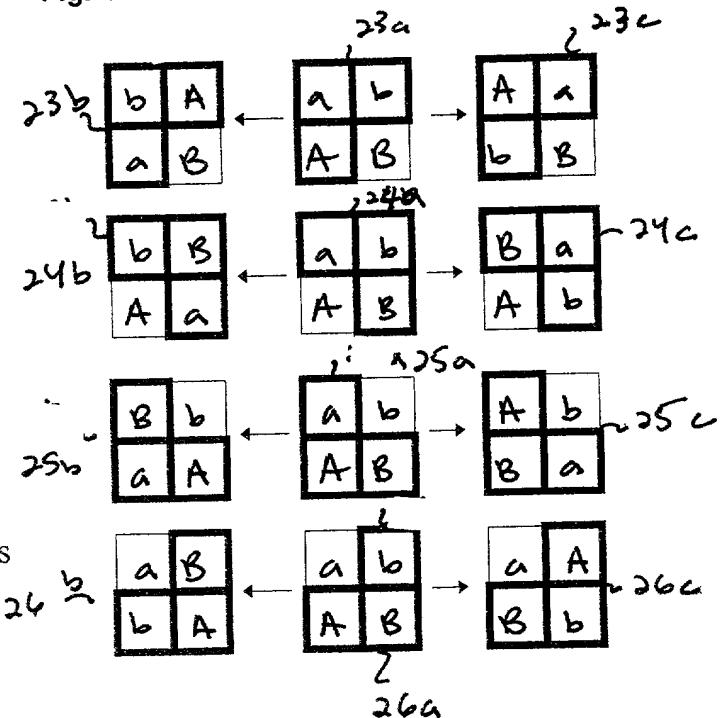
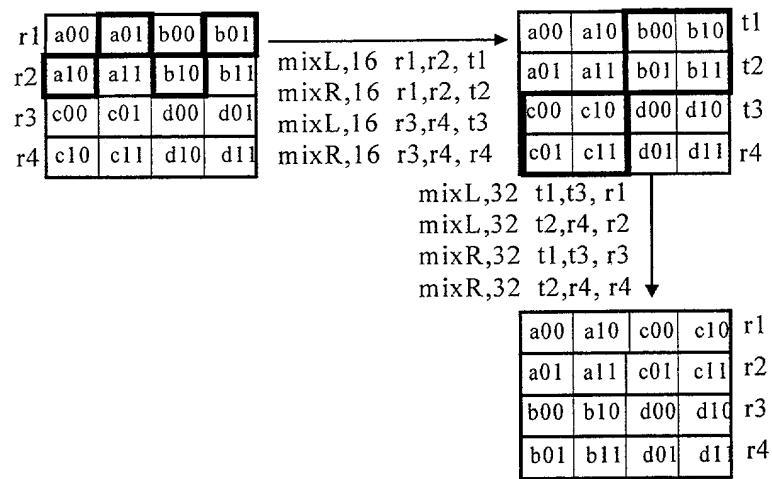


Fig. 5A

Fig. 5B

**Fig. 6:**

Identity	<table border="1"><tr><td>a</td><td>b</td></tr><tr><td>A</td><td>B</td></tr></table>	a	b	A	B					
a	b									
A	B									
Changing Rows to Diagonals	<table border="1"><tr><td>b</td><td>A</td></tr><tr><td>B</td><td>a</td></tr></table>	b	A	B	a	<table border="1"><tr><td>B</td><td>a</td></tr><tr><td>b</td><td>A</td></tr></table>	B	a	b	A
b	A									
B	a									
B	a									
b	A									
Changing Diagonals to Columns	<table border="1"><tr><td>B</td><td>A</td></tr><tr><td>a</td><td>b</td></tr></table>	B	A	a	b	<table border="1"><tr><td>A</td><td>B</td></tr><tr><td>b</td><td>a</td></tr></table>	A	B	b	a
B	A									
a	b									
A	B									
b	a									

Figure7

Alphabet A:

mixL, mixR on 8, 16 and 32 bit subwords (or **cmixL, cmixR**)
check on 8, 16 and 32-bit subwords (or **ccheck**)
excheck on 8, 16 and 32-bit subwords (or **cexcheck**)
permset on 8, 16 and 32 bit subwords, with 4-element sets (or
cexchange)

Fig. 8A

Alphabet B (minimal):

mixL, mixR on 8, 16 and 32 bit subwords (or **cmixL, cmixR**)
permset on 8, 16 and 32 bit subwords, with 4-element sets (or
cexchange)

Fig. 8B